Dakota Baber & Steven Masley

Summary

Cryptid is the next generation of identification. Cryptidate eliminates the possibility of counterfeits by adding factors of authentication and encryption that is backed a distributed global network. It benefits a group or organization of any scale by allowing them implement a secure method of managing the verification of official members.

Utilizing existing standards, such as ISO 19794-2 for our fingerprint templates and AAMVA and ANSI personal information format standards, our system can be integrated with existing software and hardware (fingerprint scanners) and easily understood. Our current version of Cryptid uses Factom as its blockchain backend. For encryption we use AES-512-CBC for data encryption and RSA-4096 for signing and verification.

Feasibility

Cryptid has been designed with scalability and feasibility in mind. A new identity costs as little as $0.05 USD, and is stored on the blockchain removing the need to handle any in house data storage (with the possibility of a breach). Because the data is on the blockchain, the maintenance cost of our software is minimal. Additional cost is only incurred if an existing ID must be modified. Since Cryptid ID strings can be stored on anything that can store 32-44 bytes of data, that means it can be implemented into current reading systems such as magstripe readers or smart card readers. Additionally, a smartphone can be used for a sort of optical data transfer -- most generally, displaying a QR code to be scanned via scanner or webcam.

Uniqueness

From the vast research we've done since beginning this project, we've found our project to be completely unique. The only organizations really focusing on any sort of secure identification were the DOD and state endorsed passports (MRTD). The problem with those systems are simply that they are not in public domain and are not as secure as Cryptid. The open nature of Cryptid allows it to be more widely adopted, adapted for security and integrated into unique systems. The use of the blockchain for immutable, effectively *unhackable*, identity storage is extremely novel and has not seen before in the industry.

Implementation and Execution

Our product is currently 100% viable and ready, and has been tested. We could serve a client and implement our verification system on top of their current infrastructure for an extremely affordable price. Once our verification system was in place, we are capable of handling any quantity of identities within minutes. Our system is also easily integrated with any current identity system, so an organization that already uses a form of identification could easily switch to Cryptid.

Need

There is need in both small and large organizations as our product is not only affordable, but also secure. The biggest advantage of Cryptid is it's complete identity security. With Cryptid identity theft is a thing of the past. A thief no longer needs only to steal your wallet to masquerade as their victim's identity. Below are three identity implementations of various security levels and their flaws compared to Cryptid:

- Rochester Institute of Technology Student Identification Cards
    - RIT, like almost every other university uses a unique number stored on the magnetic stripe for authentication. RIT in particular uses ID cards for building access, dorm access and billing. This is considered one factor of authentication and is easily susceptible to replay attack. All you need is a magnetic stripe encoder and a picture of their identification card and you have the same access as the card holder. The advantage of Cryptid in this

scenario is invulnerability to replay attacks as well as additional factors of authentication.

- United States Department of Defense Common Access Card
  - The DOD CAC uses all three factors of authentication, however the issuance of the card is limited to only DOD employees and contractors. The DOD CAC also calls back to one central database (RAPIDS -- which is vulnerable to potential data breach). The advantage of Cryptid in this scenario is the distributed nature of the block chain, further securing the data.
- ICAO Machine Readable Travel Documents (Passports)
  - Passports use two factors of authentication (something you have -- the passport -- and something you are -- the fingerprint). However, like DOD CAC they also call back to a central database. They are also far more expensive to make as they require expensive EEPROM contactless chips to store and transmit data. The advantages of Cryptid here are low cost and again the distributed nature of the block chain.

References

(2013) (1st ed.). American Association of Motor Vehicle Administrators. Retrieved from http://www.aamva.org/WorkArea/DownloadAsset.aspx?id=4435

icao.int,. (2015). *Machine Readable Travel Documents*. Retrieved 29 November 2015, from http://www.icao.int/publications/pages/publication.aspx?docnum=9303

Iso.org,. (2011). *ISO/IEC 19794-1:2011*. Retrieved 29 November 2015, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=50862

Juels, A., Molnar, D., & Wagner, D. (2005). *Security and Privacy Issues in E-passports* (1st ed.). Retrieved from http://eprint.iacr.org/2005/095.pdf

Meyer, B. (2006). *ID Replacement Project*. *rit.edu*. Retrieved 29 November 2015, from https://www.rit.edu/its/news/archive/06sept-articles/SIRP.html

Security Review of the Biometric Passport. (2005) (1st ed.). Retrieved from http://www.cs.ru.nl/~bart/TALKS/jacobs-vvss05.pdf

Van Spyk, R., Guarino, M., & Salas, A. (2008). *DoD Implementation Guide for CAC PIV End-Point*(1st ed.). U.S. Department of Defense. Retrieved from http://www.cac.mil/docs/ref1.c.i-CAC_End-Point_Implementation_Guide_v1-22.pdf